REMARKS/ARGUMENTS

This Amendment is in response to the Final Office Action date August 12, 2003. Claims 1-30 are pending. Claims 1-30 are rejected. Claims 1, 6-10, 11, 16-20, 21 and 26-30 have been amended. Accordingly, claims 1-30 remain pending in the present application.

Amended Claims

Applicant amended independent claims 1, 11 and 21 to clarify the present invention. Claims 1, 11 and 21 were amended to incorporate limitation "(c1)" recited in claims 6, 16 and 26, respectively. Claims 1, 11 and 21 now recite "generating an encryption key by the second system if the value of the first system does not match the value of the second system." Because the amendment incorporates a limitation from an existing claim, Applicant submits that no new search is required and no new matter has been presented.

Claims 6, 16 and 26 have been amended by changing claim dependencies and by deleting reference to the step of (or the means for) generating the encryption key. Claims 7-10, 17-20, and 27-30 were amended to correct claim dependencies and to make the claims consistent with one another. No new matter has been presented and a new search is not required.

35 U.S.C. §102 Rejections

The Examiner rejected claims 1-5, 11-15 and 21-25 under 35 U.S.C. §102(b) as being anticipated by Kirsch (U.S. Patent No. 5,963,915) or Luckenbaugh et al (U.S. Patent No. 6,311,269). In so doing, the Examiner stated:

> **As per claims 1, 11, and 21, Kirsch and Luckenbaugh clearly disclose a method, system, and computer readable medium for conducting a transaction over a network, the network including a first system and a second system, the method, system, and program instructions comprising the steps of:**
> **(a) initiating a transaction session;**
> **(b) comparing a value of the first system with a value of the second system, wherein the value of the first system is associated with particular**

transaction sessi n; and

(c) continuing the transacti n based on the comparison (See Kirsch abstract, figure 3 and associated text, column 3, lines 4-32, column 4, lines 48-64, and column 13, lines 15-51 and Luckenbaugh figures 2, 2B, 2C, 3 and 4 and associated text, c lumn 3, lines 35-64, column 5, liens 14-64, c lumn 7, lines 9-63, and c lumn 8, liens 1-13 and lines 53-65. To clarify both Kirsch and Luckenbaugh systems establish communication between a client and a server to retrieve certain information from a serer, once this communication is established the server checks the client for existence of a cookie if such cookie exist the server compares the cookie with existing cookies in the storage at the server. Once the cookie has been verified depending on the last transaction the cooki has been related to the transaction will continue.)

Applicant respectfully traverses.

The present invention is directed to a method and system for conducting a transaction over a network such as the Internet. Through the present invention, a customer purchasing a downloadable file over the Internet will not be charged more than once for a single file(s) if the connection to the Internet is somehow lost while the file(s) is being downloaded. According to the present invention, when the customer initiates a transaction session via a computer system, e.g., by accessing a web site and selecting a file(s) for download, the server (that supports the web site) determines whether the transaction session is a new session or one that was previously started and interrupted. The server makes this determination by comparing a value of the customer's computer system with a value of its system. (Spec. at page 4, line 17 to page 5, line 22).

If the value of the customer's computer system does *not* match the value of the server, the server will generate and store an encryption key. This key is associated with the transaction session and is used to encrypt the requested file(s). A portion of the key is then stored in the customer's system. (Spec. at page 5, lines 5-15). The value of the customer's computer system includes the portion of the key. If, on the other hand, the values match, the transaction session is one that was previously initiated but interrupted, and the server will resume the previously interrupted session. (Spec. at page 5, lines 19-22). Once the encrypted file(s) has been

downloaded successfully and the customer has paid the fee, the remaining portion of the key is provided to the customer. (Spec. at page 6, lines 6-9).

The present invention, as recited in claim 1, provides:

> 1. A method for conducting a transaction between a first system and a second system, the method comprising the steps of:
> (a) initiating a transaction session;
> (b) comparing a value of the first system with a value of the second system, wherein the value of the first system is associated with a particular transaction session; and
> (c) continuing the transaction based on the comparison by:
> (c1) generating an encryption key by the second system if the value of the first system does not match the value of the second system.

Claims 11 and 21 are system and computer product claims having scopes similar to that of claim 1.

Kirsch and Luckenbaugh are directed to methods for efficiently performing authenticated transactions between a client and a server over a network. In Kirsch, "[a] persistent predetermined coded identifier is established on the client browser corresponding to an account record stored by the merchant server." When the client wishes to purchase a product or service, the coded identifier is automatically transmitted to the merchant along with the client's selection, and the merchant "validates the predetermined coded identifier against the server stored account record." (Abstract; col. 4, lines 48-64).

Luckenbaugh is directed to implementing fine-grained access control by a user to information stored in a server. In Luckenbaugh, a value stored in a cookie is mapped to the user's identity and credentials (access privilege) stored at the server. When the user submits a request for information from the server, the server retrieves the value in the cookie, if it exists, and based on that value returns data to the user. The cookie is referred to as a security cookie and acts as a "surrogate credential" accompanying each user request during a session. (Abstract).

Applicant respectfully submits that Kirsch and Luckenbaugh fail to teach or suggest "generating an encryption key by the second system if the value of the first system does not match the value of the second system," as recited in claims 1, 11 and 21. In the present invention, the second system does *not* automatically generate the encryption key; rather it generates the encryption key if the value of the first system fails to match the value of the second system.

Neither Kirsch nor Luckenbaugh teach or suggest "generating an encryption key by the second system if the value of the first system does not match the value of the second system," as recited in claims 1, 11 and 21. Thus, Applicant respectfully submits that claims 1, 11 and 21 are allowable over Kirsch and Luckenbaugh.

Furthermore, Applicant respectfully submits that Kirsch or Luckenbaugh in view of Graunke et al. (U.S. Patent No. 5,991,399) also fails to teach or suggest "generating an encryption key by the second system if the value of the first system does not match the value of the second system," as recited in claims 1, 11 and 21. As previously stated in Applicant's response dated May 12, 2003, Graunke is directed to the "[s]ecure distribution of a private key to a user's application program (also called a 'trusted player' such as a DVD player or CD-ROM player) with conditional access based on verification of the trusted player's integrity and authenticity." (Abstract).

Graunke discloses "generating an asymmetric key pair . . . , encrypting predetermined data with the generated public key, building an executable tamper resistant key module identified for the program, the executable tamper resistant key module including the generated private key and the encrypted predetermined data, and sending the executable tamper resistant key module to the remote system. The tamper resistant key module is then executed on the remote system to check the integrity and authenticity of the program and the integrity of the tamper resistant key

module itself. If the validation process is successful, then the encrypted predetermined data is decrypted with the generated private key included in the tamper resistant key module." (Col. 3, lines 5-20).

Kirsch in combination with Graunke discloses a system whereby a client wishing to purchase digital content from a provider is authenticated via Kirsch's cookie and encryption keys for decrypting the digital content are securely transmitted to the client via Graunke's key module. Luckenbaugh in light of Graunke discloses a system that determines a user's privilege to access information in a server via Luckenbaugh's "security cookie," generates encryption keys and then securely transmits the encryption keys to the user via Graunke's key module.

In contrast to the present invention, the systems taught by the combination of Kirsch or Luckenbaugh and Graunke generate the key pair for encrypting the predetermined data either:

- after the data is *created* (Graunke, col. 8, lines 2-5; Figure 4A (step 102))
- after the program on the remote site requests the keys for decrypting the encrypted data (Gruanke, col. 7, lines 16-30; Col. 8, lines 13-20; Figure 4A (step 106))
- after the client has been authenticated, i.e., cookies match (Kirsch, step 80 Figure 3, col. 13, lines) or
- after a user's credentials have been determined (Luckenbaugh, col. 8, lines 53-65).

None of the above instances teaches or suggests "generating an encryption key if the value of the first system *does not* match the value of the second system," as recited in claims 1, 11 and 21. Accordingly, Applicant respectfully submits that claims 1, 11 and 21 are allowable over the cited references.

Claims 2-5, 12-15, and 22-25 depend on claims 1, 11 and 21, and the above arguments apply with equal force. Therefore, Applicant respectfully submits that claims 2-5, 12-15, and 22-25 are also allowable over Kirsch, Luckenbaugh and Graunke.

35 U.S.C. §103 Rejections

The Examiner rejected claims 6-10, 16-20, and 16-30 under 35 U.S.C. 103(a) as being unpatentable over Kirsch or Luckenbaugh in view of Graunke et al. (U.S. Patent No. 5,991,399). In so doing, the Examiner stated:

> **As per claims 6, 16, and 26, Kirsch and Luckenbaugh disclose all the limitations of claims 5, 15, and 25, further;**
> **Graunke clearly teaches,**
> **if the value in the cookie does not match the value in the server system, step (c) further comprises:**
> - **(c1) generating an encryption key;**
> - **(c2) storing a portion of the encryption key in the cookie; and**
> - **(c3) storing the entire encryption key on the server system (See Graunke abstract, figures 2, 4A and 4B and associated text, column 3, lines 5-20 and 60-68, column 6, lines 17-35, column 7, lines 8-68, and column 8, lines 1-31). . . .**
>
> **As per claims 9, 19, and 29, Kirsch and Luckenbaugh disclose all the limitations of claims 5, 15, and 25, further;**
> **Graunke clearly teaches, if the value in the cookie does match the value in the server system, ABC discloses that step (c) further comprises:**
> - **(c1) allowing the server system to transfer encrypted information to the client system; and**
> - **(c2) allowing the server system to transfer a remaining portion of the encryption key to the client system whereby the encryption key is capable of being utilized by the client system to decrypt the encrypted information (see Graunke abstract, figures 2, 4A and 4B and associated text, column 3, lines 5-20 and 60-68, column 6, lines 17-35, column 7, lines 8-68, and column 8, lines 1-31).**

Applicant respectfully submits that claims 6-10, 16-20, and 16-30 depend on claims 1, 11 and 21, respectively, and the arguments regarding claims 1, 11 and 21 apply with equal force. As such, claims 6-10, 16-20, and 16-30 are allowable over the cited references.

Applicant also submits that claims 6-10, 16-20, and 16-30 are allowable for independent and additional reasons, which have been presented in Applicant's previous response dated May 12, 2003, and are hereby incorporated herein by reference in their entirety. In summary, those reasons include:

1. Graunke fails to teach or suggest "storing a first portion of the encryption key in the first system," as recited in claims 6, 16 and 26.

2. Graunke fails to teach or suggest "allowing the second system to transfer *a remaining portion* of the encryption key to the first system," as recited in claims 7, 9, 17, 19, 27 and 29 because all of the keys in Graunke's key module are complete public or private keys.

3. Claims 8, 10, 18, 20, 28 and 30 depend on claims 7, 9, 17, 19, 27 and 29, respectively, and therefore the above arguments apply with equal force.

Conclusion

In view of the foregoing, it is submitted that the claims 1-30 are allowable over the cited references and are in condition for allowance. Applicant respectfully requests reconsideration of the rejections and objections to the claims, as now presented.

Applicant believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

November 3, 2003
Date

Joyce Tom
Attorneys for Applicant(s)
Reg. No.: 48,681
(650) 493-4540